(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 April 2003 (10.04.2003)

PCT

(10) International Publication Number
WO 03/029940 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/US02/26092

(22) International Filing Date: 15 August 2002 (15.08.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/969,686 2 October 2001 (02.10.2001) US

(71) Applicant *(for all designated States except US)*: NETWORKS ASSOCIATES TECHNOLOGY, INC. [US/US]; 3965 Freedom Circle, Santa Clara, CA 95054 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: SINGLETON, Richard, B. [GB/GB]; 4 Coral Close, Eaton Bray, Bedfordshire LU6 2AS (GB).

(74) Agents: MALLIE, Michael, J. et al.; Blakely, Sokoloff, Taylor & Zafman LLP, 12400 Wilshire Boulevard, 7th floor, Los Angeles, CA 90025 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 03/029940 A2

(54) Title: MASTER SECURITY POLICY SERVER

(57) Abstract: A master policy server manages security polices for client computers through a network of local policy servers. Each local policy server is responsible for the security policies on a group of clients and maintains a data store containing the security policies and security information pertaining to the clients. Periodically, the master policy server and the local policy server synchronize, at which time the master policy server replicates updated policies to the local policy servers and the policy servers upload client security statistics to the master policy server for consolidation into a global status.

MASTER SECURITY POLICY SERVER

FIELD OF THE INVENTION

This invention relates generally to computer security, and more particularly to managing security policies through a centralized server.

COPYRIGHT NOTICE/PERMISSION

BACKGROUND OF THE INVENTION

Organizations often manage their computer security policies from a central location, typically employing a single computer server to manage the security polices on networked user (client) computers. The clients poll the server several times a day to check for, and optionally download, updated security policies and to upload their status to the server. Assuming a client and the server exchange a large amount of data several times a day, the data traffic between the server and even a small number clients can cause significant degradation for overall network communications.

SUMMARY OF THE INVENTION

A master policy server manages security polices for client computers through a network of local policy servers. Each local policy server is responsible for the security policies on a group of clients and maintains a data store containing the security policies and security information pertaining to the clients. Periodically, the master policy server and the local policy server synchronize, at which time the master policy server replicates

updated policies to the local policy servers and the local policy servers upload client security statistics to the master policy server for consolidation into a global status. A local policy server may also request an updated security policy outside of the synchronization timeframe. Similarly, the master policy server may also request the client statistics from a local policy server outside of the synchronization timeframe.

Because the local policy servers consolidate the statistics from the clients prior to uploading it to the master policy server, the amount of data flowing through the network to the master policy server is greatly reduced. Similarly, because the master policy server replicates the security policies to a few local policy servers instead of to each client, the amount of data flowing through the network from the master policy server is also reduced.

The present invention describes systems, clients, servers, methods, and computer-readable media of varying scope. In addition to the aspects and advantages of the present invention described in this summary, further aspects and advantages of the invention will become apparent by reference to the drawings and by reading the detailed description that follows.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a diagram illustrating a system-level overview of an embodiment of the invention;

Figure 2A is a flowchart of a method to be performed by a master server according to an embodiment of the invention;

Figure 2B is a flowchart of a method to be performed by a local server operating in conjunction with the master server of Figure 2A;

Figure 3A is a diagram of one embodiment of an operating environment suitable for practicing the present invention; and

Figure 3B is a diagram of one embodiment of a computer system suitable for use in the operating environment of Figure 3A.

DETAILED DESCRIPTION OF THE INVENTION

In the following detailed description of embodiments of the invention, reference is made to the accompanying drawings in which like references indicate similar elements, and in which is shown by way of illustration specific embodiments in which the invention may be practiced. These embodiments are described in sufficient detail to enable those skilled in the art to practice the invention, and it is to be understood that other embodiments may be utilized and that logical, mechanical, electrical, functional, and other changes may be made without departing from the scope of the present invention. The following detailed description is, therefore, not to be taken in a limiting sense, and the scope of the present invention is defined only by the appended claims.

A system level overview of the operation of an embodiment of the invention is described by reference to Figure 1, which illustrates a security policy distribution system 100. The system 100 utilizes a master policy server 101 to manage security policies on client (user) computers through a network 129 of local policy severs A 103, B 105 and C 107. For example, local policy server A103 manages client A-1 115 through client A-N 117, while local policy server B 105 manages client B-1 119 through B-N 121. Although the clients are represented as individual systems in Figure 1, it will be appreciated that they may be grouped together by hardware and software platform type, domain name, site location, or physical or logical region.

Each local policy server has a local data store 109, 111, 113 that contains the security policies and security information collected from the client computers it manages. Each type of hardware and software platform acting as a client computer may be associated with a exemplary security policy or may share exemplary security policies with other platforms. The security policy may contain configuration parameters for anti-virus programs, firewalls, and other security software that protect a client computer from compromise by a third-party.

Communication between the local policy servers 103, 105, 107 and the master policy server 101 through network 129 is intermittent. Each local policy server 103, 105, 107 is responsible for periodically querying the master policy server 101 to determine if the security policies applicable to its clients have changed. The local policy servers also periodically, or upon request, send client security statistics derived from the security

information on local data stores 109, 111, 113 to the master policy server 101, which acts as a consolidation point for status information regarding the overall security of the system 100. The statistics from the local policy servers are stored in a global data store 127. When a global status for the system 100 is requested, the master policy server 101 derives the status from the statistics in the global data store 127 and, optionally, from additional statistics obtained from the local policy servers. More detailed status information for particular clients or groups of clients is obtained from the appropriate local policy server.

In one embodiment, the master policy server 101 and the local policy servers 103, 105, 107 synchronize security policies and statistics at times when less data traffic is generally experienced on the network 129. When the local policy servers are physically located in different time zones, the synchronization may occur at several points during a twenty-four hour period. In an alternate embodiment, the local policy servers can schedule checks for updated policies in addition to the synchronization process. Furthermore, it will be appreciated that the synchronization at a local policy server may happen more than once a day. The network 129 connecting the master policy server and the local policy servers is secured using any of several well-known secure transmission protocols when the security policies are being uploaded to the master policy server 101 or replicated to the local policy servers 103, 105, 107. Otherwise, no particular network transmission protocols are required in the system 100.

When the system 100 is installed, the system administrator may create the initial security policies at one of the local policy servers 103, 105, 107 for transfer to the master policy server 101 and subsequent replication to the other local policy servers, or directly at the master policy server 101. Similarly, updates to the security policies may be performed at a local policy server or at the master policy server. In one embodiment, the master policy server 101 maintains global level security policy configurations and the local policy servers 103, 105, 107 derive their local level configuration and set-up policies for their clients from the global level configurations.

The number of local policy servers is dependent upon the number of clients at each site and the physical locations of the sites. Because the master policy server 101 only sends and receives data from the local policy servers 103, 105, 107 instead of each

of the clients, a single master policy server and common TCP/IP wide-area networks are generally able to handle the amount of data being transferred in the system 100. Alternate embodiments in which additional levels of servers are incorporated between the local policy servers 103,105, 107 and the master policy server 101 are also contemplated and are considered within the scope of the invention.

The operations of an embodiment of a security policy distribution system 100 have been described in terms of a single master policy server and three local policy servers as illustrated in Figure 1, but the invention is not so limited. Next, the particular methods of the invention that perform the operations for the system 100 are described in terms of computer software with reference to a series of flowcharts. The methods to be performed by a computer constitute computer programs made up of computer-executable instructions illustrated as blocks (acts). Describing the methods by reference to a flowchart enables one skilled in the art to develop such programs including such instructions to carry out the methods on suitably configured computers (the processing unit of the computer executing the instructions from computer-readable media). The computer-executable instructions may be written in a computer programming language or may be embodied in firmware logic. If written in a programming language conforming to a recognized standard, such instructions can be executed on a variety of hardware platforms and for interface to a variety of operating systems. In addition, the present invention is not described with reference to any particular programming language. It will be appreciated that a variety of programming languages may be used to implement the teachings of the invention as described herein. Furthermore, it is common in the art to speak of software, in one form or another (e.g., program, procedure, process, application, module, logic...), as taking an action or causing a result. Such expressions are merely a shorthand way of saying that execution of the software by a computer causes the processor of the computer to perform an action or a produce a result.

Referring first to Figure 2A, the acts to be performed by a computer executing a master server method 200 to perform the operations described for the master policy server 101 in Figure 1 is shown. The master server method 200 is invoked by one or more of a series of predetermined events. If a new policy has been created, either at the master policy server 101, or at one of the local policy servers, 103, 105, 107, (block 201),

the master server method 200 obtains and stores the security policy at block 203. If the master server method 200 receives a request for a new policy from a local policy server (block 205), the master server method 200 replicates the policy to the requestor at block 207. It will be appreciated that the master policy server will replicate those policies which are requested by the local policy server, i.e., those policies particular to the client platforms which the local policy server is managing. If the master server method 200 receives a request for system status (block 209), the master server method 200 determines if the request is for historical or current status (block 213). If the report is for current status, the master server method 200 obtains the current statistics from the local servers at block 215. The appropriate status is returned to the requester at the block 217. Otherwise, the event that invoked the master server method 200 is a scheduled synchronization event and the master server method 200 synchronizes security policies and statistics with the appropriate local policy servers at block 211.

A local server method 230 is illustrated in Figure 2B that performs the operations previously described for the local policy servers 103, 105, 107 in Figure 1. As with the master server method 200, the local server method 230 is invoked by one or more of a predetermined sequence of events. If a new policy has been configured on the local policy server (block 231), the local server method 230 sends the new policy to the master policy server at block 233 for replication to the other local policy servers. If the event is a scheduled check for the availability of new policies (block 235), the local server method 230 requests appropriate new policies from the master policy server at block 237 and receive and apply any new policies at block 239. If the local server method 230 receives a request for current status from the master server method 200 (block 241), it send its current statistics to the master policy server at block 243. Otherwise, the event is a scheduled synchronization event and the local server method 230 synchronizes with the master policy server at block 245, sending statistics from the local data store to the master policy server and receiving any updates to the security policies.

The methods performed by a master policy server and local policy server have been shown by reference to flowcharts in Figures 2A and 2B, respectively, including all the acts from 201 until 217 and from 231 until 245. It will be appreciated that more or fewer processes may be incorporated into the methods illustrated in Figures 2A-B

without departing from the scope of the invention, and that no particular order is implied by the arrangement of blocks shown and described herein.

The following description of Figures 3A-B is intended to provide an overview of computer hardware and other operating components suitable for performing the methods of the invention described above, but is not intended to limit the applicable environments. One of skill in the art will immediately appreciate that the invention can be practiced with other computer system configurations, including hand-held devices, multiprocessor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers, and the like. The invention can also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network.

Figure 3A shows several computer systems that are coupled together through a network 3, such as the Internet. The term "Internet" as used herein refers to a network of networks which uses certain protocols, such as the TCP/IP protocol, and possibly other protocols such as the hypertext transfer protocol (HTTP) for hypertext markup language (HTML) documents that make up the World Wide Web (web). The physical connections of the Internet and the protocols and communication procedures of the Internet are well known to those of skill in the art. Access to the Internet 3 is typically provided by Internet service providers (ISP), such as the ISPs 5 and 7. Users on client systems, such as client computer systems 21, 25, 35, and 37 obtain access to the Internet through the Internet service providers, such as ISPs 5 and 7. Access to the Internet allows users of the client computer systems to exchange information, receive and send e-mails, and view documents, such as documents which have been prepared in the HTML format. These documents are often provided by web servers, such as web server 9 which is considered to be "on" the Internet. Often these web servers are provided by the ISPs, such as ISP 5, although a computer system can be set up and connected to the Internet without that system being also an ISP as is well known in the art.

The web server 9 is typically at least one computer system which operates as a server computer system and is configured to operate with the protocols of the World Wide Web and is coupled to the Internet. Optionally, the web server 9 can be part of an ISP which provides access to the Internet for client systems. The web server 9 is shown

coupled to the server computer system 11 which itself is coupled to web content 10, which can be considered a form of a media database. It will be appreciated that while two computer systems 9 and 11 are shown in Figure 3A, the web server system 9 and the server computer system 11 can be one computer system having different software components providing the web server functionality and the server functionality provided by the server computer system 11 which will be described further below.

Client computer systems 21, 25, 35, and 37 can each, with the appropriate web browsing software, view HTML pages provided by the web server 9. The ISP 5 provides Internet connectivity to the client computer system 21 through the modem interface 23 which can be considered part of the client computer system 21. The client computer system can be a personal computer system, a network computer, a Web TV system, or other such computer system. Similarly, the ISP 7 provides Internet connectivity for client systems 25, 35, and 37, although as shown in Figure 3A, the connections are not the same for these three computer systems. Client computer system 25 is coupled through a modem interface 27 while client computer systems 35 and 37 are part of a LAN. While Figure 3A shows the interfaces 23 and 27 as generically as a "modem," it will be appreciated that each of these interfaces can be an analog modem, ISDN modem, cable modem, satellite transmission interface (e.g. "Direct PC"), or other interfaces for coupling a computer system to other computer systems. Client computer systems 35 and 37 are coupled to a LAN 33 through network interfaces 39 and 41, which can be Ethernet network or other network interfaces. The LAN 33 is also coupled to a gateway computer system 31 which can provide firewall and other Internet related services for the local area network. This gateway computer system 31 is coupled to the ISP 7 to provide Internet connectivity to the client computer systems 35 and 37. The gateway computer system 31 can be a conventional server computer system. Also, the web server system 9 can be a conventional server computer system.

Alternatively, as well-known, a server computer system 43 can be directly coupled to the LAN 33 through a network interface 45 to provide files 47 and other services to the clients 35, 37, without the need to connect to the Internet through the gateway system 31.

Figure 3B shows one example of a conventional computer system that can be used as a client computer system or a server computer system or as a web server system. It will also be appreciated that such a computer system can be used to perform many of the functions of an Internet service provider, such as ISP 5. The computer system 51 interfaces to external systems through the modem or network interface 53. It will be appreciated that the modem or network interface 53 can be considered to be part of the computer system 51. This interface 53 can be an analog modem, ISDN modem, cable modem, token ring interface, satellite transmission interface (e.g. "Direct PC"), or other interfaces for coupling a computer system to other computer systems. The computer system 51 includes a processing unit 55, which can be a conventional microprocessor such as an Intel Pentium microprocessor or Motorola Power PC microprocessor. Memory 59 is coupled to the processor 55 by a bus 57. Memory 59 can be dynamic random access memory (DRAM) and can also include static RAM (SRAM). The bus 57 couples the processor 55 to the memory 59 and also to non-volatile storage 65 and to display controller 61 and to the input/output (I/O) controller 67. The display controller 61 controls in the conventional manner a display on a display device 63 which can be a cathode ray tube (CRT) or liquid crystal display. The input/output devices 69 can include a keyboard, disk drives, printers, a scanner, and other input and output devices, including a mouse or other pointing device. The display controller 61 and the I/O controller 67 can be implemented with conventional well known technology. A digital image input device 71 can be a digital camera which is coupled to the I/O controller 67 in order to allow images from the digital camera to be input into the computer system 51. The non-volatile storage 65 is often a magnetic hard disk, an optical disk, or another form of storage for large amounts of data. Some of this data is often written, by a direct memory access process, into memory 59 during execution of software in the computer system 51. One of skill in the art will immediately recognize that the term "computer-readable medium" includes any type of storage device that is accessible by the processor 55 and also encompasses a carrier wave that encodes a data signal.

It will be appreciated that the computer system 51 is one example of many possible computer systems which have different architectures. For example, personal computers based on an Intel microprocessor often have multiple buses, one of which can

be an input/output (I/O) bus for the peripherals and one that directly connects the processor 55 and the memory 59 (often referred to as a memory bus). The buses are connected together through bridge components that perform any necessary translation due to differing bus protocols.

Network computers are another type of computer system that can be used with the present invention. Network computers do not usually include a hard disk or other mass storage, and the executable programs are loaded from a network connection into the memory 59 for execution by the processor 55. A Web TV system, which is known in the art, is also considered to be a computer system according to the present invention, but it may lack some of the features shown in Figure 3B, such as certain input or output devices. A typical computer system will usually include at least a processor, memory, and a bus coupling the memory to the processor.

It will also be appreciated that the computer system 51 is controlled by operating system software which includes a file management system, such as a disk operating system, which is part of the operating system software. One example of an operating system software with its associated file management system software is the family of operating systems known as Windows® from Microsoft Corporation of Redmond, Washington, and their associated file management systems. The file management system is typically stored in the non-volatile storage 65 and causes the processor 55 to execute the various acts required by the operating system to input and output data and to store data in memory, including storing files on the non-volatile storage 65.

A security policy distribution system that is managed by a master security policy server has been described. Although specific embodiments have been illustrated and described herein, it will be appreciated by those of ordinary skill in the art that any arrangement which is calculated to achieve the same purpose may be substituted for the specific embodiments shown. This application is intended to cover any adaptations or variations of the present invention.

The terminology used in this application with respect to network communications is meant to include all communication media and environments, including local and wide area networks, public and private communications environments, and wired and wireless

communications media. Therefore, it is manifestly intended that this invention be limited only by the following claims and equivalents thereof.

CLAIMS

What is claimed is:

1. A computerized method of distributing security policies comprising:
maintaining a security policy at a master policy server; and
periodically synchronizing the master policy server and a local policy server to replicate the security policy at the local policy server.

2. The computerized method of claim 1, wherein the synchronizing further comprises obtaining security statistics from the local policy server by the master policy server.

3. The computerized method of claim 2 further comprising:
deriving a global status from the statistics.

4. The computerized method of claim 1, further comprising:
obtaining security statistics by the master policy server upon request to the local policy server.

5. The computerized method of claim 1 further comprising:
replicating the security policy to the local policy server upon request to the master policy server.

6. The computerized method of claim 1 further comprising:
creating the security policy at the local policy server; and
transferring the security policy to the master policy server.

7. The computerized method of claim 1 further comprising:
creating the security policy at the master policy server.

8. The computerized method of claim 1, wherein the synchronizing is performed securely across a communications medium coupling the master policy server and the local policy server.

9. The computerized method of claim 1, further comprising:

managing security for a plurality of client platforms by the local policy server, the security policy comprising security parameters particular to each client platform.

10. The computerized method of claim 9, further comprising:

deriving the security policy parameters particular to each client platform from global security parameters, the security policy at the master policy comprising the global security parameters.

11. A computer-readable medium having executable instructions to cause a computer to perform a method comprising:

maintaining a security policy at a master policy server; and

periodically synchronizing the master policy server and a local policy server to replicate the security policy at the local policy server.

12. The computer-readable medium of claim 11, wherein the synchronizing further comprises obtaining security statistics from the local policy server by the master policy server.

13. The computer-readable medium of claim 12, wherein the method further comprises:

deriving a global status from the statistics.

14. The computer-readable medium of claim 11, wherein the method further comprises:

obtaining security statistics by the master policy server upon request to the local policy server.

15. The computer-readable medium of claim 11, wherein the method further comprises:

replicating the security policy to the local policy server upon request to the master policy server.

16. The computer-readable medium of claim 11, wherein the method further comprises:

creating the security policy at the local policy server; and

transferring the security policy to the master policy server.

17. The computer-readable medium of claim 11, wherein the method further comprises:

creating the security policy at the master policy server.

18. The computer-readable medium of claim 11, wherein the synchronizing is performed securely across a communications medium coupling the master policy server and the local policy server.

19. The computer-readable medium of claim 11, wherein the method further comprises:

managing security for a plurality of client platforms by the local policy server, the security policy comprising security parameters particular to each client platform.

20. The computer-readable medium of claim 19, wherein the method further comprises:

deriving the security policy parameters particular to each client platform from global security parameters, the security policy at the master policy comprising the global security parameters.

21. A computer system comprising:

a processor coupled to a memory through a bus;

a network interface coupled to the processor through the bus; and

a master server process executed from the memory by the processor to cause the processor to maintain a security policy and to periodically synchronize with a local policy server through the network interface to replicate the security policy at the local policy server.

22. The computer system of claim 21, wherein the master server process further causes the processor to obtain security statistics from the local policy server through the network interface during synchronization.

23. The computer system of claim 22, wherein the master server process further causes the processor to derive a global status from the statistics.

24. The computer system of claim 21, wherein the master server process further causes the processor to request security statistics from the local policy server through the network interface.

25. The computer system of claim 21, wherein the master server process further causes the processor to receive a request from the local policy server and to replicate the security policy to the local policy server in response.

26. The computer system of claim 21, wherein the master server process further causes the processor to create the security policy.

27. The computer system of claim 21, wherein the master server process further causes the processor to couple the network interface to a secure communications medium for synchronization.

28. A computer system comprising:

a processor coupled to a memory through a bus;

a network interface coupled to the processor through the bus; and

a local server process executed from the memory by the processor to cause the processor to periodically synchronize with a master policy server through the network interface to receive a security policy from a master policy server.

29. The computer system of claim 28, wherein the local server process further causes the processor to transfer security statistics to the master policy server through the network interface during synchronization.

30. The computer system of claim 28, wherein the local server process further causes the processor to receive a request for security statistics from the master policy server and to transfer the security statistics to the master policy server through the network interface in response.

31. The computer system of claim 28, wherein the local server process further causes the processor to request a security policy from the master policy server through the network interface and to receive the security policy in response.

32. The computer system of claim 28, wherein the local server process further causes the processor to create the security policy and to transfer the security policy to the master policy server through the network interface.

33. The computer system of claim 28, wherein the local server process further causes the processor to manage security for a plurality of client platforms, the security policy comprising security parameters particular to each client platform.

34. The computer system of claim 33, wherein the local server process further causes the processor to derive the security policy parameters particular to each client platform from global security parameters, the security policy at the master policy server comprising the global security parameters.

35. An apparatus comprising:

network means for interfacing to a network; and

master policy means for maintaining a security policy and for periodically synchronizing with a local policy means through the network interface to replicate the security policy at the local policy means.

36. The apparatus of claim 35, wherein the master policy means is further operable for obtaining security statistics from the local policy means through the network means during synchronization.

37. The apparatus of claim 36, wherein the master policy means is further operable for deriving a global status from the statistics.

38. The apparatus of claim 35, wherein the master policy means is further operable for requesting security statistics from the local policy means through the network means.

39. The apparatus of claim 35, wherein the master policy means is further operable for receiving a request from the local policy means through the network means and for replicating the security policy to the local policy means through the network means in response.

40. The apparatus of claim 35, wherein the master policy means is further operable for creating the security policy.

41. The apparatus of claim 35, wherein the network means is further operable for coupling to a secure communications medium for synchronization between the master policy means and the local policy means.

42. An apparatus comprising:

network means for interfacing to a network; and

local policy means for periodically synchronizing to a master policy means through the network means to receive a security policy form the master policy means.

43. The apparatus of claim 42, wherein the local policy means is further operable for transferring security statistics to the master policy means through the network means during synchronization.

44. The apparatus of claim 42, wherein the local policy means is further operable for receiving a request for security statistics from the master policy means through the network means and for transferring the security statistics to the master policy means through the network means in response.

45. The apparatus of claim 42, wherein the local policy means is further operable for requesting a security policy from the master policy means through the network means and for receiving the security policy from the master policy means through the network means in response.

46. The apparatus of claim 42, wherein the local policy means is further operable for creating the security policy and for transferring the security policy to the master policy means through the network means.

47. The computer system of claim 42, wherein the local security means is further operable for managing security for a plurality of client platforms, the security policy comprising security parameters particular to each client platform.

48. The computer system of claim 47, wherein the local security means is further operable for deriving the security policy parameters particular to each client platform from global security parameters, the security policy at the master policy means comprising the global security parameters.

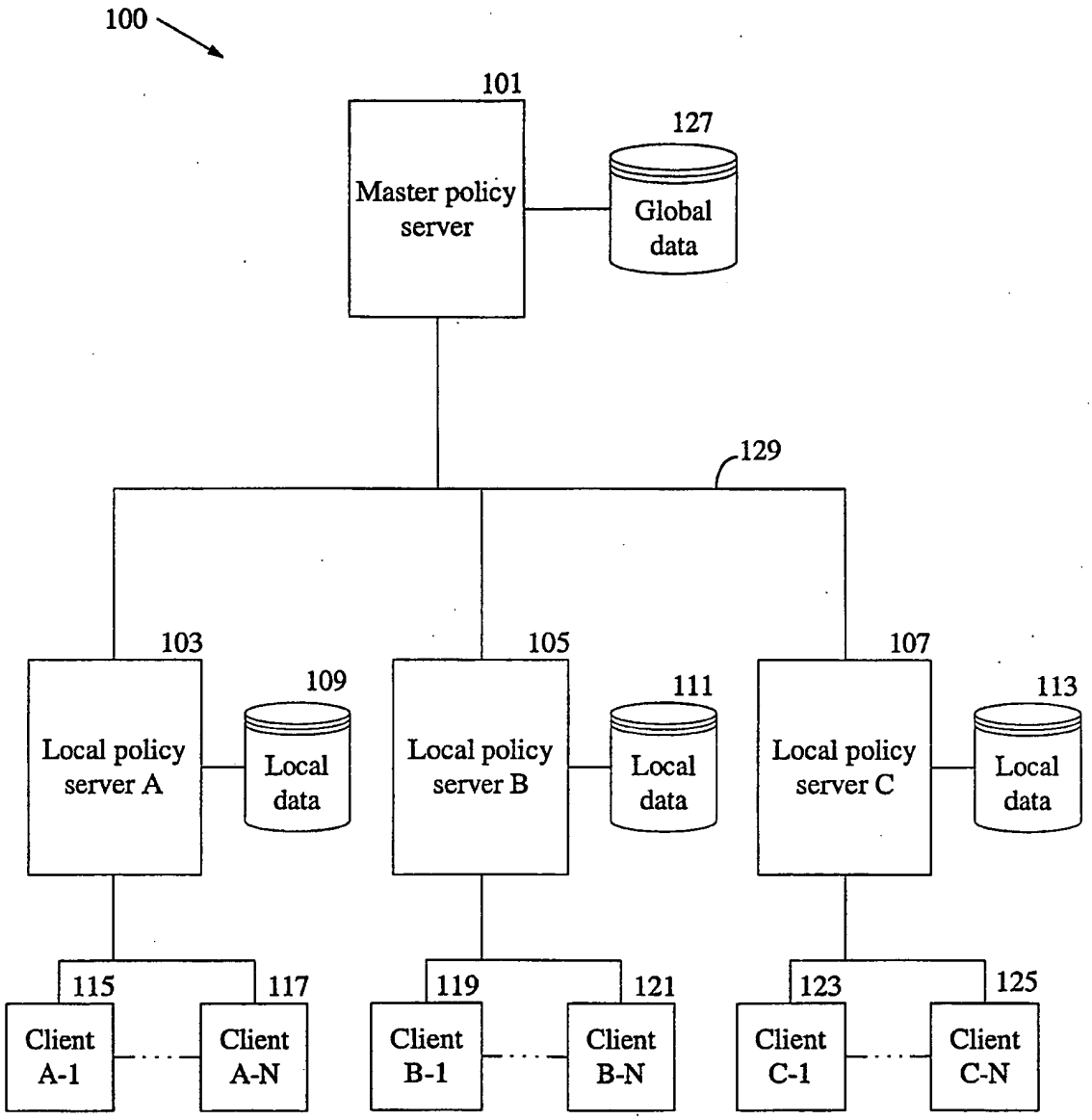
100
101
Master policy server
127
Global data
129
103
Local policy server A
109
Local data
105
Local policy server B
111
Local data
107
Local policy server C
113
Local data
115
Client A-1
117
Client A-N
119
Client B-1
121
Client B-N
123
Client C-1
125
Client C-N

Figure 1

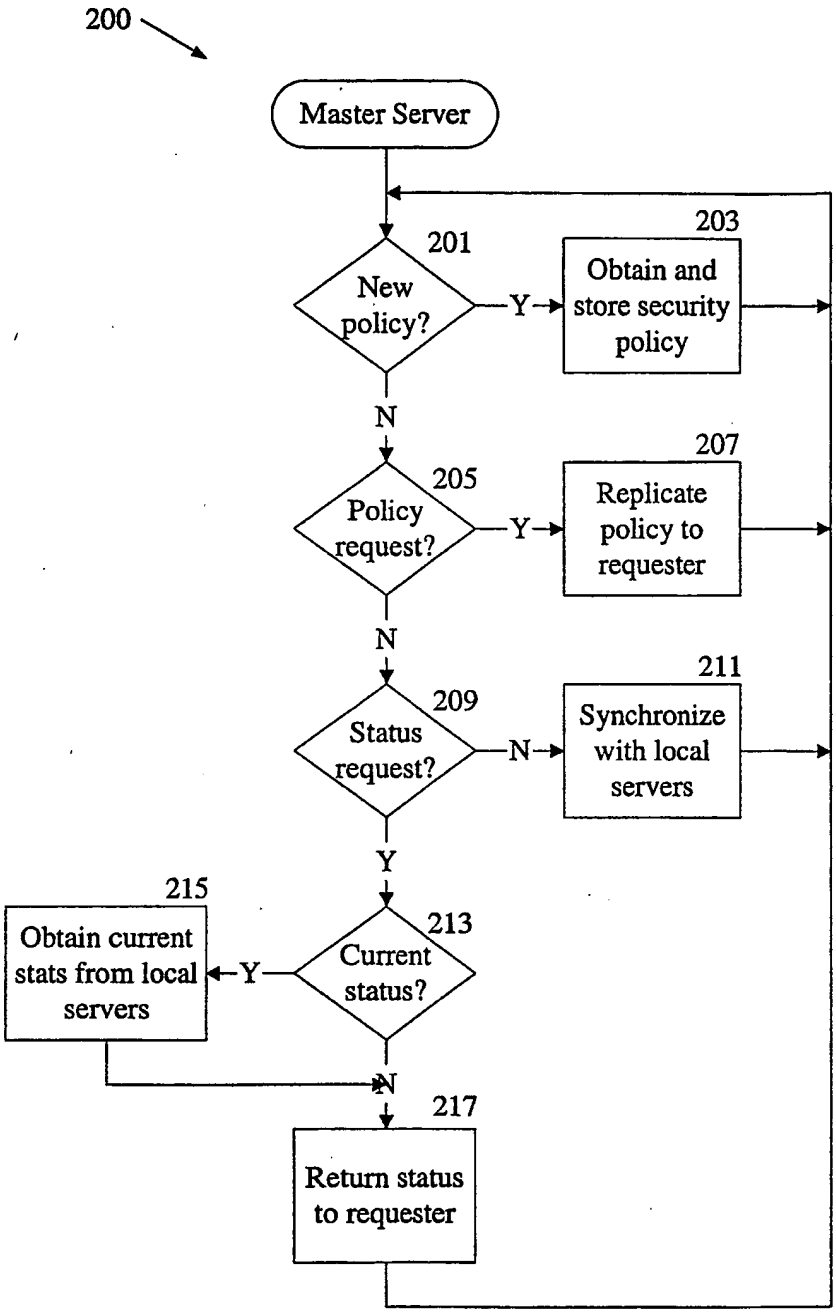
200
Master Server
201
New policy?
Y
203
Obtain and store security policy
N
205
Policy request?
Y
207
Replicate policy to requester
N
209
Status request?
N
211
Synchronize with local servers
Y
213
Current status?
Y
215
Obtain current stats from local servers
N
217
Return status to requester

Figure 2A

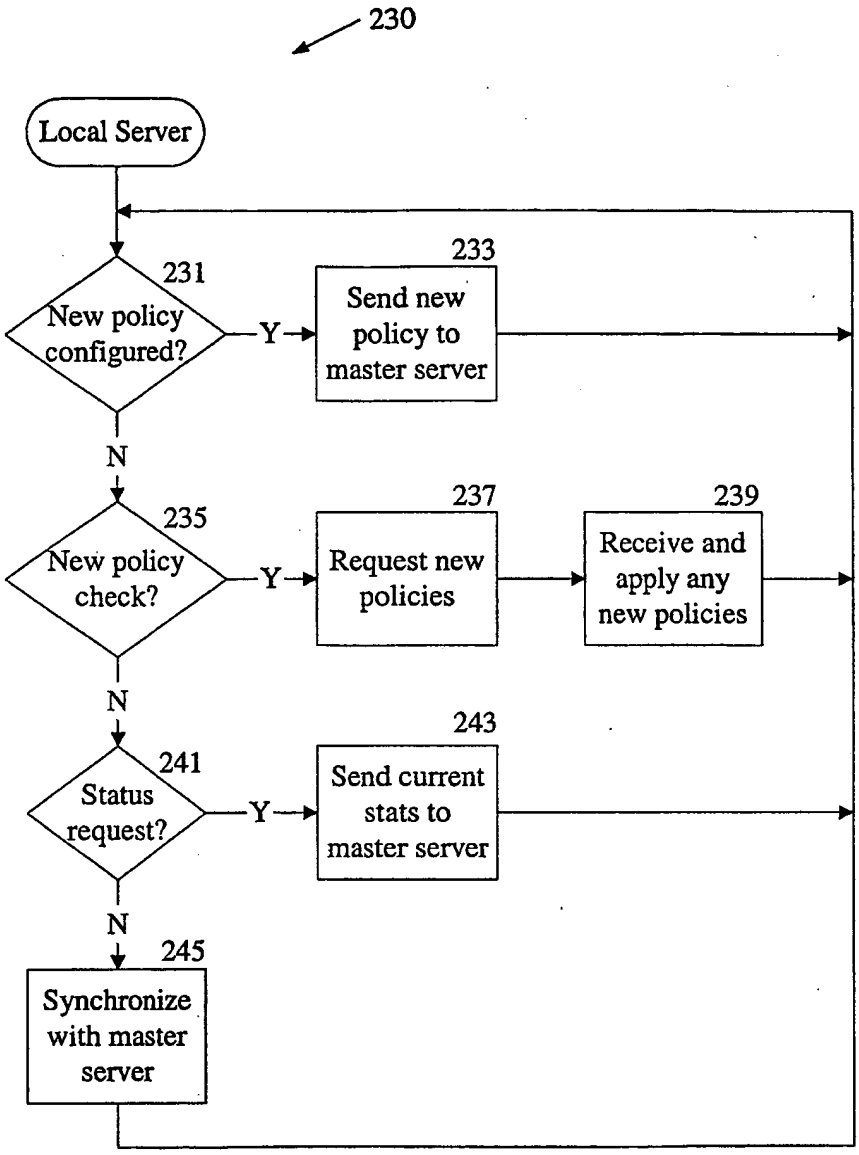
230
Local Server
231
New policy configured?
Y
233
Send new policy to master server
N
235
New policy check?
Y
237
Request new policies
239
Receive and apply any new policies
N
241
Status request?
Y
243
Send current stats to master server
N
245
Synchronize with master server

Figure 2B

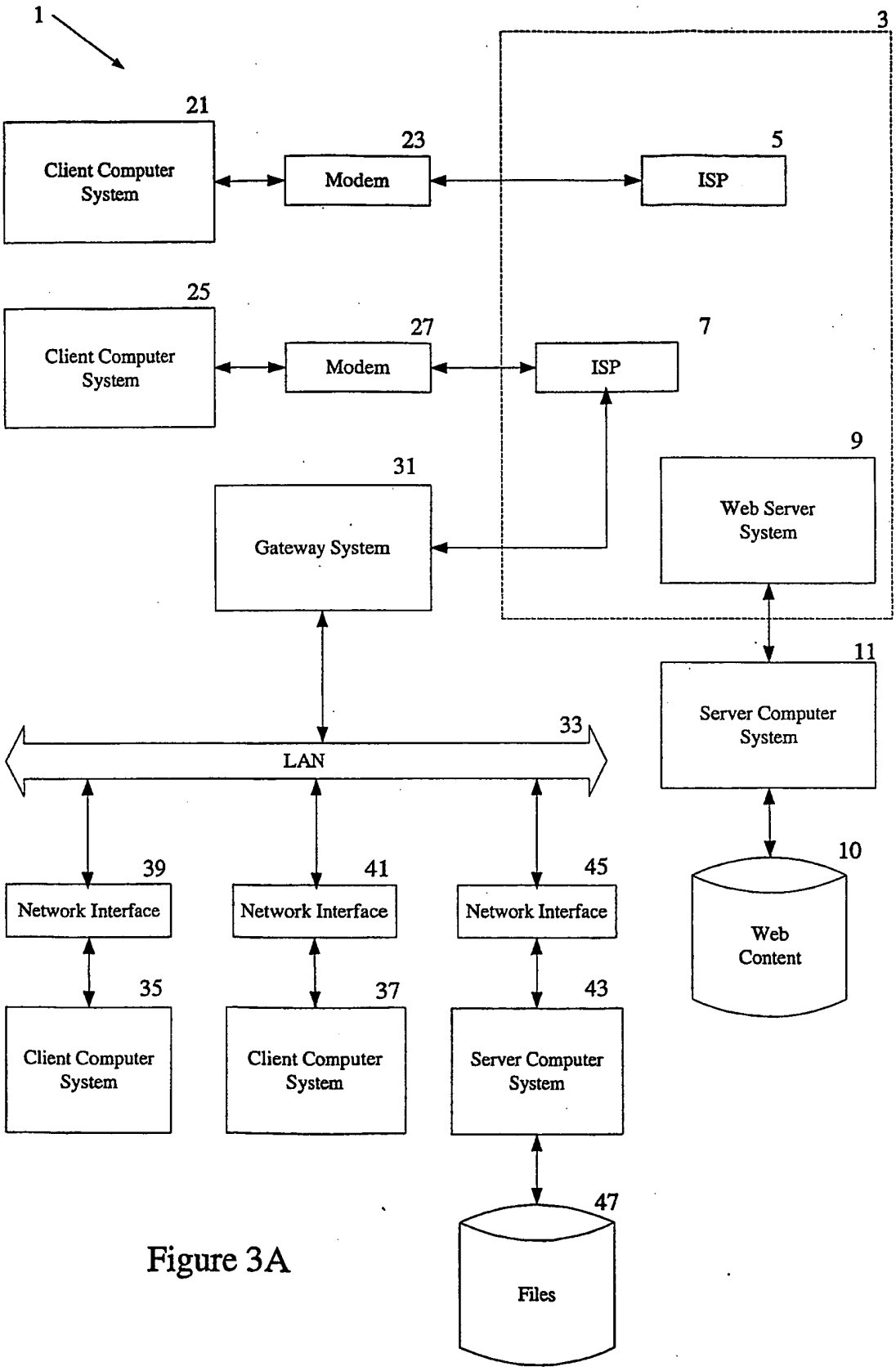
1
3
21
Client Computer System
23
Modem
5
ISP
25
Client Computer System
27
Modem
7
ISP
9
Web Server System
31
Gateway System
11
Server Computer System
33
LAN
39
Network Interface
41
Network Interface
45
Network Interface
10
Web Content
35
Client Computer System
37
Client Computer System
43
Server Computer System
47
Files

Figure 3A

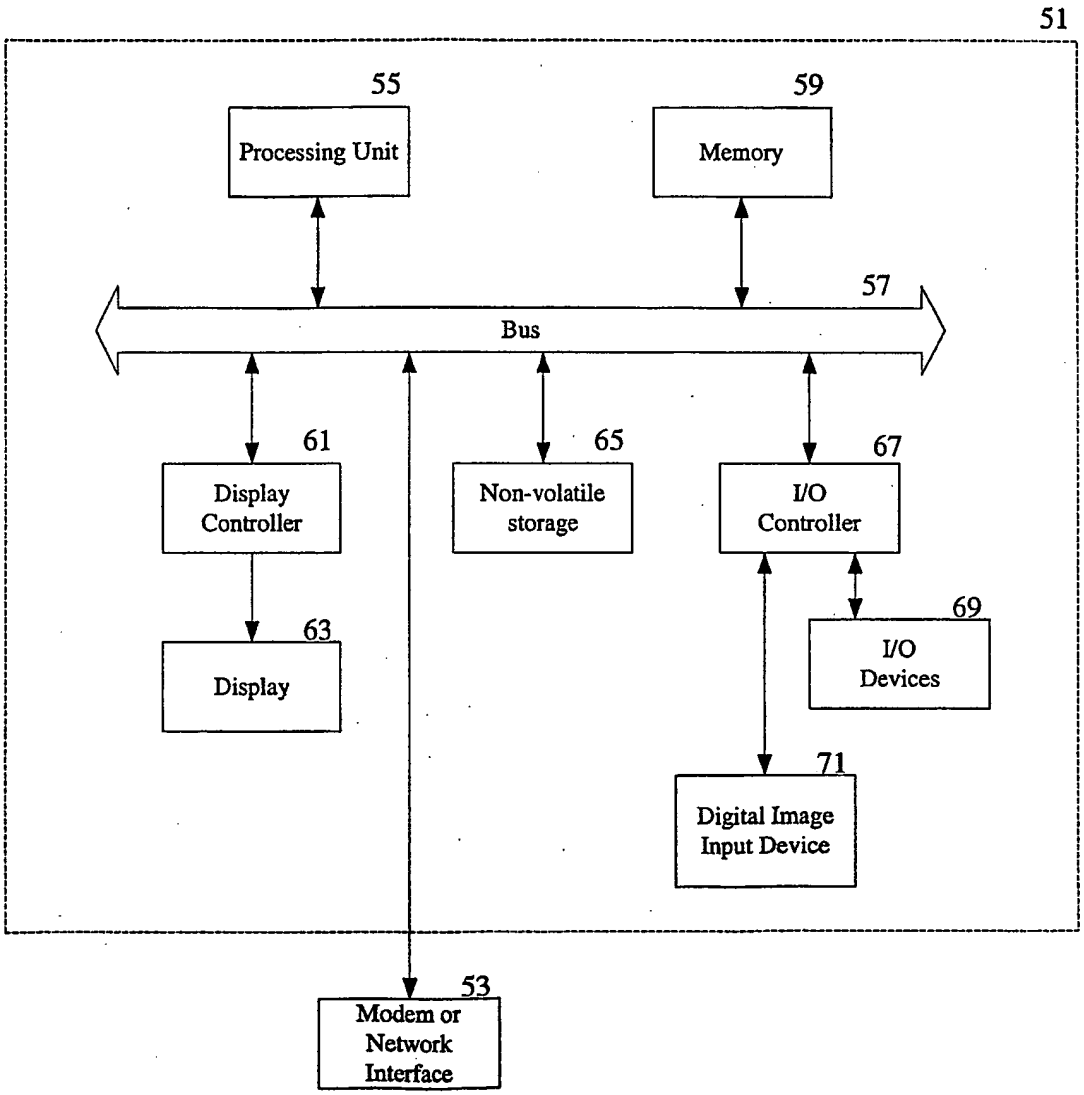
51
55
Processing Unit
59
Memory
57
Bus
61
Display Controller
63
Display
65
Non-volatile storage
67
I/O Controller
69
I/O Devices
71
Digital Image Input Device
53
Modem or Network Interface

Figure 3B